POLÍTICA DE CONTROLE INTERNO, RISCOS E COMPLIANCE

FESTOR INSTITUIÇÃO DE PAGAMENTO 2026

POLÍTICA DE CONTROLE INTERNO, RISCOS E COMPLIANCE

Festor Instituição de Pagamento Ltda.

ASSUNTO	VERSÃO	PUBLICADA EM	PRÓXIMA REVISÃO
Política de Controle Interno, Riscos e Compliance	4.0	14/08/2026	14/08/2027

ÁREA DE APLICAÇÃO	ELABORADOR	APROVADORES	CLASSIFICAÇÃO DA INFORMAÇÃO
Todas as áreas	Compliance / Controles Internos e Riscos	Diretoria Executiva	Interna – Pública

CÓDIGO DO DOCUMENTO: COD-CI-001-2026-V4.0

Histórico de Revisão

EDIÇÃO	VERSÃO	DATA	TIPO (I/E/A/N)	SUMÁRIO DE ALTERAÇÃO
2023	1.0	20/03/2023	N	Estruturação inicial como Política de Controles Internos & Compliance
2024	2.0	04/07/2024	I / A	Reestruturação como Manual de Controles Internos, com metodologia de Matriz de Riscos e Controles (MRC), alinhada à Resolução BCB nº 260/2022
2024	3.0	16/08/2024	A	Revisão periódica da metodologia de controles internos
2026	4.0	14/08/2026	I / A	Fusão das versões anteriores em documento único; atualização de razão social, CNPJ e endereço para Festor Instituição de Pagamento Ltda.; incorporação dos processos de compliance (segregação de atividades, conflito de interesses, KYC, PLD/FT, anticorrupção, confidencialidade, treinamentos) à estrutura de controles internos; padronização de canais de contato e alinhamento visual com o padrão de governança do Festor.

LEGENDA DO HISTÓRICO DE REVISÃO – TIPO DE ALTERAÇÃO

ABREVIATURA	DESCRIÇÃO
I	*Inclusão: Inclusão de informação não existente na versão anterior.*
E	*Exclusão: Exclusão de informação existente na versão anterior.*
A	*Alteração ou ajuste de informação já existente na versão anterior.*
N	*Novo: Indica a data em que o normativo foi criado, que corresponde à primeira versão do documento.*

Sumário

1. Objetivo

O termo compliance origina-se do verbo inglês "to comply", que significa cumprir, obedecer, executar e satisfazer aquilo que foi imposto ou definido. Compliance é, portanto, o dever de estar em conformidade e fazer cumprir as leis, regulamentos internos e externos, processos, procedimentos, políticas e diretrizes, visando à mitigação do risco legal e dos riscos relacionados à reputação.

O Festor Instituição de Pagamento Ltda. ("Festor"), em conformidade com as resoluções e circulares expedidas pelo Banco Central do Brasil (BACEN), apresenta esta Política de Controle Interno, Riscos e Compliance ("Política"), elaborada de acordo com as normas vigentes e as boas práticas de mercado, com a finalidade de firmar as regras, procedimentos e mecanismos que assegurem e viabilizem o permanente atendimento às normas e regulamentações vigentes referentes às atividades desenvolvidas pelo Festor e aos padrões éticos e profissionais aplicáveis.

Complementarmente a esta Política, deve ser também observado e respeitado o Código de Ética e Conduta do Festor, bem como as demais políticas específicas mencionadas ao longo deste documento.

2. Aplicação

Esta Política é aplicável a todos os Administradores, Diretores, Colaboradores, estagiários e prestadores de serviços do Festor, independentemente do cargo, função ou área de atuação, bem como a parceiros comerciais na medida em que interajam com as atividades reguladas do Festor.

3. Base Legal

Norma	Descrição
Resolução BCB nº 260/2022	Dispõe sobre os sistemas de controles internos das instituições de pagamento autorizadas a funcionar pelo Banco Central do Brasil.
Resolução BCB nº 65/2021	Dispõe sobre a política de conformidade (compliance) das instituições de pagamento autorizadas a funcionar pelo Banco Central do Brasil.
Resolução CMN nº 4.968/2021	Dispõe sobre a política de controles internos a ser adotada pelas instituições financeiras; utilizada como referência comparativa e alinhada aos princípios da metodologia COSO adotados nesta Política.
Resoluções BCB nº 197 e nº 198/2022	Classificam os conglomerados prudenciais liderados por instituição de pagamento ("Tipo 2") e dispõem sobre a estrutura de gerenciamento contínuo de riscos e o requerimento mínimo de Patrimônio de Referência de Instituição de Pagamento (PRIP) aplicáveis ao Festor.
Lei nº 12.846/2013 (Lei Anticorrupção)	Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira.
Lei nº 9.613/1998	Dispõe sobre os crimes de lavagem ou ocultação de bens, direitos e valores, e cria o Conselho de Controle de Atividades Financeiras (COAF).
Lei nº 13.709/2018 (LGPD)	Lei Geral de Proteção de Dados Pessoais, que regula o tratamento de dados pessoais no Brasil.
Lei nº 12.965/2014 (Marco Civil da Internet)	Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil.
Código de Ética e Conduta do Festor	Documento interno complementar que estabelece os princípios éticos e as regras de conduta aplicáveis a todos os Colaboradores.

4. Definições

Termo	Definição
Sistema de Controles Internos	Conjunto de políticas, normas, procedimentos e atividades estabelecidas pelo Festor com o propósito de reduzir a possibilidade de sofrer perdas financeiras e desgaste da imagem institucional, incrementar a qualidade das informações contábeis, financeiras e gerenciais, e salvaguardar a conformidade com a legislação e a regulamentação em vigor.
Controle	Atividade que visa evitar perdas de qualquer natureza, assim como desvios dos objetivos de um processo, corrigindo desvios em relação aos propósitos gerais ou específicos previamente estabelecidos.
COSO	Committee of Sponsoring Organizations of the Treadway Commission — organização dedicada à melhoria dos relatórios financeiros por meio da aplicação da ética e da efetividade no cumprimento dos controles, possibilitando monitorar o alcance dos objetivos organizacionais frente aos riscos identificados.
Gerenciamento de Riscos	Processo para identificar, avaliar, administrar e controlar potenciais eventos ou situações, para fornecer razoável certeza quanto ao alcance dos objetivos organizacionais.
Risco	Evento futuro identificado, ao qual é possível associar uma probabilidade de ocorrência e a qualificação da incerteza com relação ao rumo dos acontecimentos planejados. Compreende todo fator, interno ou externo, que possa afetar adversamente os objetivos da organização.
Risco de Compliance	Risco de sanções regulatórias, perda financeira ou perda de reputação, resultantes de falhas no cumprimento de leis, códigos de conduta, regulamentações, autorregulamentações, políticas e procedimentos internos.
Risco Operacional	Possibilidade de perdas decorrentes da execução inadequada de processos internos, pessoas ou sistemas, ou de eventos externos, incluindo erros, fraudes e falhas operacionais.
Conflito de Interesses	Situação em que um Colaborador está envolvido em duas ou mais atividades ou relacionamentos incompatíveis, de modo que sua conduta possa conflitar com sua função no Festor ou afetar seu julgamento e desempenho.
Informação Privilegiada	Informação relevante e material a respeito de qualquer companhia, produto e/ou serviço, que não tenha sido divulgada publicamente e que tenha sido obtida de forma privilegiada, em decorrência de relação profissional ou pessoal.
Instituição do Tipo 2	Conglomerado prudencial cuja instituição líder seja uma Instituição de Pagamento e que não seja integrada por instituição financeira ou por outra instituição autorizada a funcionar pelo BACEN — categoria em que o Festor se enquadra, nos termos das Resoluções BCB nº 197 e nº 198/2022.

5. Diretrizes

O Festor busca manter uma estrutura de controles internos alinhada com as melhores práticas de Governança Corporativa e com os normativos emanados dos órgãos reguladores.

A área de Controles Internos deve prover garantias de que as informações financeiras e gerenciais são confiáveis e completas, e de que o Festor está aderente às diversas políticas, regulamentações e legislações aplicáveis. Seu principal objetivo é prevenir, podendo tornar-se a mais importante proteção para a organização.

Para que o Sistema de Controles Internos seja eficaz, é essencial que todos os Colaboradores reconheçam a importância de exercer suas atribuições com eficiência, informando às áreas competentes quaisquer

problemas de que tenham conhecimento, como casos de descumprimento de normas internas ou externas.

5.1 Modelo de Três Linhas de Defesa

O modelo de Gerenciamento de Riscos do Festor baseia-se no conceito do "Modelo de Três Linhas" de atuação, alinhado à estrutura organizacional:

Linha de Defesa	Composição e Atribuições
1ª Linha	Áreas executivas representadas por seus gestores (negócios e suporte), que devem estabelecer e implementar controles visando monitorar e avaliar os riscos potenciais relacionados aos seus processos, possuindo propriedade sobre eles e sendo responsáveis por implementar ações corretivas.
2ª Linha	Áreas de Gestão de Riscos, Compliance e Controles Internos, independentes da gestão das linhas de negócios, que atuam no monitoramento periódico do desenho e funcionamento dos controles, fornecendo suporte e avaliação sobre a qualidade dos controles internos e do gerenciamento de riscos.
3ª Linha	Auditoria Interna, responsável pela revisão independente do gerenciamento de riscos, apoiando a organização a atingir seus objetivos por meio de abordagem sistemática e disciplinada para avaliar e aprimorar a eficácia dos processos de gestão de riscos, controles e governança, fornecendo à Diretoria Executiva avaliações baseadas no maior nível de independência e objetividade.

5.2 Governança de Compliance

A responsabilidade direta pelas atividades relacionadas a controles internos e compliance é atribuição do responsável por Compliance do Festor, que atua em conjunto com o Comitê de Compliance e Riscos.

São funções do responsável por Compliance:

- Acompanhar e atualizar os códigos, diretrizes, políticas, procedimentos e controles internos;
- Certificar a aderência e o cumprimento das leis, regulamentações, instruções e normas emitidas pelos órgãos reguladores e autorreguladores relativas às atividades do Festor;
- Assegurar a adequação dos Colaboradores aos códigos, diretrizes, políticas, procedimentos e controles internos;
- Garantir que o relacionamento entre Colaboradores, sócios, clientes, concorrentes, fornecedores e prestadores de serviço esteja em conformidade com as leis, regulamentações e políticas internas;
- Levar pedidos de autorização, orientação, esclarecimento ou casos de ocorrência, suspeita ou indício de prática em desacordo com esta Política para apreciação do Comitê de Compliance e Riscos;
- Assegurar a adequada segregação de atividades a fim de evitar conflitos de interesse;
- Identificar possíveis condutas contrárias a esta Política;
- Assessorar o gerenciamento dos negócios quanto à interpretação e impacto da legislação, monitorando as melhores práticas e analisando periodicamente as normatizações emitidas pelo BACEN e demais órgãos reguladores;
- Convocar e organizar as reuniões do Comitê de Compliance e Riscos, sempre que julgar necessário;
- Preservar a identidade de Colaboradores que reportem qualquer conduta ilegal, antiética ou contrária a esta Política, garantindo que não sofrerão consequências negativas devido ao comunicado; e
- Disseminar a cultura de controles internos e compliance para assegurar o cumprimento de leis e regulamentos existentes.

São atribuições do Comitê de Compliance e Riscos:

- Definir os princípios éticos a serem observados por todos os Colaboradores do Festor;

- Promover a ampla divulgação e aplicação dos preceitos éticos, inclusive por meio de treinamentos;
- Apreciar todos os casos que cheguem ao seu conhecimento sobre potencial descumprimento dos preceitos de compliance previstos nesta Política ou nas demais políticas internas, inclusive situações não previstas;
- Garantir o sigilo de eventuais denunciantes de delitos ou infrações, exceto nos casos de necessidade de testemunho judicial;
- Solicitar, sempre que julgar necessário, o apoio da auditoria interna ou externa ou de outra assessoria especializada;
- Tratar todos os assuntos que cheguem ao seu conhecimento com o mais absoluto sigilo, preservando os interesses e a imagem institucional do Festor, bem como dos envolvidos;
- Definir eventuais penalidades a Colaboradores, quando julgar necessário; e
- Analisar situações que possam ser caracterizadas como conflito de interesse pessoal e profissional.

6. Sistema de Controles Internos

O Sistema de Controles Internos visa garantir a existência de uma Estrutura de Controles na organização que permita a compreensão dos principais riscos decorrentes de fatores internos e externos, assegurando que esses riscos sejam identificados, avaliados, monitorados, controlados e testados de forma eficiente e eficaz.

A finalidade do Sistema de Controles Internos é permitir que o Festor possua razoável garantia quanto à mitigação dos riscos que permeiam as operações e as atividades críticas do seu negócio. O Sistema de Controles Internos compreende: a Estrutura de Controles; a Matriz de Riscos e Controles (MRC); o Plano de Ação; o Teste de Controles; e o Relatório de Efetividade do Sistema de Controles Internos.

6.1 Estrutura de Controles

A Estrutura de Controles pode ser definida como o conjunto de políticas, normas, procedimentos e atividades estabelecidas com o propósito de reduzir a possibilidade de sofrer perdas financeiras e desgaste da imagem institucional, incrementar a qualidade das informações contábeis, financeiras e gerenciais, e salvaguardar a conformidade com a legislação e a regulamentação em vigor.

Uma estrutura de controles pode ser considerada eficiente e eficaz se a Diretoria Executiva tiver segurança razoável de que: o objetivo das operações está sendo alcançado; as demonstrações financeiras são preparadas de maneira confiável; as operações estão em conformidade com os normativos internos; e as leis e regulamentos aplicáveis estão sendo cumpridos.

6.2 Montagem da Estrutura de Controles

A montagem da Estrutura de Controles tem como princípio a identificação e a classificação dos riscos que podem atuar adversamente no negócio do Festor. A área de Gestão de Riscos, por meio de entrevistas com as áreas de negócios, efetua a identificação dos riscos inerentes à operação e a classificação dos riscos com foco na mitigação e na efetividade dos controles.

A identificação dos riscos visa garantir que a Estrutura de Controles esteja alinhada com os principais riscos decorrentes das atividades, e que potenciais deficiências identificadas sejam corrigidas. No momento da identificação, é feita uma classificação preliminar conforme a probabilidade de ocorrência e o impacto causado caso o risco se materialize. A classificação final do risco é dada pelas informações obtidas junto ao gestor da área de negócio e pela eficiência do controle apresentado.

6.3 Matriz de Riscos e Controles (MRC)

Entende-se por controle o conjunto de políticas, normas e metodologia, além de atividades de acompanhamento, automatizadas ou não, com vistas a reduzir o grau de exposição a risco, subsidiar o cumprimento dos objetivos estabelecidos, assegurar a conformidade com leis e regulamentos, e promover a confiabilidade dos relatórios gerenciais.

O controle está diretamente ligado à redução da incerteza com relação a eventos futuros: quanto melhor o controle, menor o risco. Tendo como base os riscos identificados, o profissional da área de Controles Internos define e descreve o controle que irá mitigar a ocorrência do risco. A Matriz de Riscos e Controles é composta pelas seguintes informações: Processo; Risco; Avaliação do Risco; Controle; e Avaliação do Controle.

6.3.1 Identificação dos Processos

Esse grupo abrange: identificação sequencial (numeração dentro da matriz); identificação do macroprocesso; e identificação do processo.

6.3.2 Identificação dos Riscos

O Festor se enquadra nas regras relativas ao gerenciamento de riscos e governança aplicáveis a Instituições do Tipo 2 (conglomerado prudencial cuja instituição líder seja uma Instituição de Pagamento não integrada por instituição financeira), descritas nas Resoluções BCB nº 197 e nº 198/2022.

Esse grupo abrange: o número do risco identificado, associado à atividade operacional; a descrição do risco; a categorização do risco segundo o BACEN; o evento do risco (tipo de evento relacionado à categoria); e a área responsável pelo risco ("dono" do processo). As categorias de risco segundo o BACEN são:

- Risco Operacional: decorre da possibilidade de perdas resultantes de eventos externos ou de falha, deficiência ou inadequação de processos internos, pessoas ou sistemas;
- Risco de Liquidez: decorre da possibilidade de o Festor não ser capaz de honrar eficientemente suas obrigações correntes e futuras sem afetar suas operações diárias e sem incorrer em perdas significativas, ou de não ser capaz de converter moeda eletrônica em moeda física ou escritural no momento da solicitação do usuário;
- Risco de Crédito: como Instituição de Pagamento, o Festor não tem autorização para conceder crédito caracterizado como privilégio de instituições financeiras, observando apenas riscos de crédito com clientes e contrapartes decorrentes de operações de meios de pagamento e de investimentos;
- Risco de Conformidade (Compliance): decorre da possibilidade de o Festor sofrer sanções legais ou administrativas, perdas financeiras, danos de reputação e outros danos, decorrentes de descumprimento ou falhas na observância do arcabouço legal, da regulamentação infralegal, das recomendações dos órgãos reguladores e dos códigos de autorregulação aplicáveis;
- Risco Cibernético: decorre da possibilidade de perdas associadas a falhas em procedimentos de segurança cibernética, tais como autenticação, mecanismos de rastreabilidade, controles de acesso, testes de vulnerabilidade e prevenção de vazamento de informações;
- Risco Socioambiental e Climático: decorre da possibilidade de perdas resultantes de danos socioambientais e efeitos climáticos negativos gerados ou sofridos pelas atividades econômicas do Festor;
- Risco de Gerenciamento de Capital: decorre da possibilidade de perdas resultantes do gerenciamento ineficiente do capital mantido pelo Festor em relação ao nível necessário para fazer face aos riscos a que está exposto e ao seu planejamento estratégico — tratado em documento específico que apresenta a metodologia aplicada, as responsabilidades e os procedimentos para controle e manutenção do capital aos níveis exigidos pelo BACEN, nos termos das Resoluções BCB nº 197 e nº 198/2022.

6.3.3 Avaliação e Classificação dos Riscos

Avaliação do Risco é o processo de comparação dos resultados da análise do risco com os critérios de risco para determinar sua magnitude. Classificação do Risco é o método utilizado para categorizar e avaliar os riscos aos quais o Festor está sujeito, envolvendo a identificação dos riscos, a avaliação de sua probabilidade de ocorrência e de seu impacto, e a classificação de acordo com sua gravidade — permitindo uma visão clara dos riscos e a tomada de medidas para preveni-los ou mitigá-los.

Classificação	Impacto do Risco
Baixo	Perdas irrelevantes ou pequenas perdas setoriais que não afetam a imagem da empresa. Perdas financeiras até R$ 50.000,00 (até 0,3% do lucro líquido do ano anterior).
Médio	Perdas pontuais ou conjunto de perdas materiais setorizadas que afetam de alguma forma a lucratividade e/ou comprometem passageiramente a imagem da empresa. Perdas financeiras entre R$ 50.000,00 e R$ 500.000,00 (0,3% a 1% do lucro líquido do ano anterior).
Alto	Perdas que acarretam acentuado declínio da lucratividade e/ou produzem desgastes marcantes à imagem da empresa. Perdas financeiras acima de R$ 500.000,00 (acima de 1% do lucro líquido do ano anterior).

Classificação	Probabilidade do Risco
Baixo	Ocorrência do evento no prazo de até 1 (um) ano.
Médio	Ocorrência do evento no prazo de até 3 (três) meses.
Alto	Ocorrência do evento no prazo de até 1 (uma) semana.

A Classificação do Risco (Risco Inerente) é apurada em função do Impacto versus a Probabilidade, com pesos atribuídos: Impacto — Alto = 3, Médio = 2, Baixo = 1; Probabilidade — Alta = 3, Média = 2, Baixa = 1. O Risco Inerente resultante (Impacto × Probabilidade) é classificado como Alto, Médio ou Baixo conforme a matriz de apuração adotada pelo Festor.

6.3.4 Identificação e Estabelecimento de Controles

Esse grupo abrange o conjunto de atributos de controle:

- Tipo de Controle — Operacional: oferece a linha de frente de defesa para prevenção, detecção e correção de erros (ex.: conciliações, relatórios de exceção, limites de transação, controles de acesso); Monitoramento: assegura que todos os demais controles funcionem conforme desenhados (ex.: revisão de métricas de desempenho, observação de controles operacionais); ou não se aplica, quando não há forma de medir;
- Descrição do Controle: detalha como o controle associado à atividade é executado;
- Frequência de execução: Anual, Semestral, Trimestral, Bimestral, Mensal ou Diário;
- Natureza do Controle: Detectivo (visa mitigar a severidade de um evento já ocorrido), Preventivo (age sobre a probabilidade de ocorrência de um evento, impedindo que aconteça), ou não se aplica;
- Forma de Execução: Automático (executado por meio de sistemas) ou manual.

6.3.5 Nível de Controle

Esse grupo abrange:

- Eficiência — capacidade de gerenciamento e produção de efeito, avaliando a qualidade das atividades controladas: Baixa (controle inexistente, não reconhecido ou reconhecido, mas não gerenciado; ações corretivas apenas reativas); Média (risco mitigado, controles suficientes, mas validação apenas no âmbito da gestão, com ações preventivas parcialmente implementadas); Alta (risco medido e mitigado, com administração e gerências participando ativamente, estrutura formalizada e atuação preventiva);
- Eficácia — grau de sucesso nos resultados alcançados: Baixa (processos e controles existem, mas podem não estar sendo aplicados corretamente, sem monitoramento adequado); Média (processos definidos, mas não totalmente implantados por ferramentas adequadas); Alta (processos, sistemas e controles implantados com ferramentas adequadas, permitindo monitoramento integrado por indicadores de desempenho e de risco).

6.3.6 Apuração do Nível de Controle

O Nível do Controle é a pontuação dos indicadores em função da Eficácia versus a Eficiência, por meio de parâmetros estabelecidos: Eficácia — Alta = peso 3, Média = peso 2, Baixa = peso 1; Eficiência — Alta = peso 3, Média = peso 2, Baixa = peso 1. O resultado do Nível de Controle é classificado como Alto, Médio ou Baixo, conforme a matriz de apuração adotada pelo Festor.

6.3.7 Risco Residual

O Risco Residual é a conjunção dos dados apurados pelo Risco Inerente versus o Nível de Controle. A resposta ao Risco Residual deve estabelecer alçadas para sua solução, considerando os seguintes critérios:

- Risco Alto e Médio: a solução deve ser proposta pelo Gestor responsável e aprovada pelo Diretor da respectiva área. Em caso de discordância entre o Gestor da área e a área de Controles Internos, a resposta deverá ser aprovada pelo Comitê de Compliance e Riscos;
- Risco Baixo: a solução pode ser proposta e aprovada pelo Gestor responsável.

O Festor deve estabelecer prazos e responsáveis pela execução dos Planos de Ação em relação aos Riscos Residuais, com o objetivo de mitigá-los, observando os seguintes prazos:

- Risco Alto: até 30 (trinta) dias;
- Risco Médio: até 60 (sessenta) dias;
- Risco Baixo: sem prazo de ação obrigatório.

6.4 Plano de Ação

O Plano de Ação consiste em um conjunto de estratégias, tarefas e prazos elaborado visando atingir um determinado resultado associado aos riscos identificados, com o objetivo de tratar a deficiência. O Plano deve conter: a data de verificação da efetividade do controle; texto descrevendo a situação atual e o plano de ação para tratar a deficiência identificada; o prazo para implantação do novo controle; a área e o gestor responsáveis; e o status da implantação.

6.5 Testes de Controles — Monitoramento

Os testes de controles/monitoramento consistem no processo de verificação, supervisão, observação crítica e implantação de melhorias a partir da identificação de mudanças no nível de desempenho requerido ou esperado, sendo realizados periodicamente pela área de Controles Internos e anualmente pela Auditoria Interna.

É importante que o monitoramento do Sistema de Controles Internos garanta: que os pontos de controle sejam eficazes e eficientes; que os limites/alçadas e as regulamentações vigentes estejam sendo cumpridos; que eventuais desvios identificados estejam sendo corrigidos e os controles reavaliados; que haja aprimoramento contínuo do processo; e que haja acompanhamento de mudanças no contexto externo e interno.

Os testes de controles são efetuados principalmente para os riscos classificados como Médio e Alto, quando serão solicitadas aos responsáveis evidências amostrais para verificar se os controles são realmente eficientes. São considerados aceitáveis os riscos classificados como Baixo que não acarretem perda financeira; os riscos Baixos que acarretem perda financeira deverão ter seus controles testados para verificar sua efetividade.

Todos os testes realizados são documentados, podendo ser solicitado plano de ação para melhorar o controle e trazer os riscos a um nível aceitável. Será considerado eficiente o controle cuja evidência apresentada esteja completa e em conformidade com o controle descrito na Matriz de Riscos e Controles.

A planilha de Testes de Controles deve conter: data do monitoramento; tipo de monitoramento (reunião, walkthrough ou coleta sistemática); tipo de checagem (coleta de evidência, teste por observação, exame, indagação ou amostragem); efetividade (Efetivo, Necessidade de Melhorias, ou inadequado); e consequência efetiva (sanções regulatórias, prejuízo de imagem, desvantagem competitiva, prejuízo financeiro, perda de receita, informações contábeis/gerenciais incorretas, ou nenhuma).

6.6 Demonstrativo da Efetividade do Sistema de Controles Internos

Cabe à área de Controles Internos elaborar o "Relatório de Controles Internos" a fim de avaliar a efetividade do Sistema de Controles. O Relatório deve: ser elaborado anualmente, com data-base de 31 de dezembro; ser encaminhado para ciência e aprovação da Diretoria Executiva até 31 de março do ano seguinte à data-base; e permanecer à disposição do Banco Central do Brasil pelo prazo de 5 (cinco) anos.

O Relatório deve descrever a forma e o resultado dos testes efetuados, incluindo recomendações pertinentes à formulação dos planos de ação para tratar as deficiências identificadas. O Relatório compreende: a metodologia adotada na avaliação da efetividade; os testes aplicados aos controles; as deficiências identificadas; a avaliação dos procedimentos destinados a conhecer os clientes (KYC); a avaliação dos procedimentos de monitoramento, seleção, análise e comunicação ao COAF de operações e situações suspeitas; a avaliação das medidas de desenvolvimento da cultura organizacional voltadas à prevenção à lavagem de dinheiro e ao financiamento do terrorismo; e a avaliação dos procedimentos destinados a conhecer Colaboradores, parceiros e prestadores de serviços terceirizados.

Compete aos gestores das áreas de negócios a elaboração de Planos de Ação destinados a solucionar as deficiências identificadas. Compete à área de Controles Internos monitorar e fazer o follow-up da implementação desses planos, registrando o resultado no relatório "Monitoramento — Planos de Ação", direcionado à Diretoria Executiva. A revisão dos riscos e da estrutura de controles internos, bem como a implementação dos planos de ação junto às áreas responsáveis, são atividades executadas anualmente.

6.7 Principais Controles

Controles Contábeis e Administrativos:

- Registros contábeis e administrativos quanto às transações realizadas;
- Integração entre o sistema interno operacional e o sistema contábil, permitindo detecção tempestiva de eventuais diferenças entre os saldos apresentados;
- Realização de operações devidamente registradas no tempo oportuno;
- Produção de relatórios de controle para acompanhamento dos valores das operações, saldos, receitas, despesas, vencimentos e apropriações, em conformidade com os termos e condições negociados com clientes;
- Realização das operações em conformidade com os limites estabelecidos nas políticas internas;
- Ordenação das operações e seu respectivo processamento, observando-se a adequada segregação de responsabilidades;
- Garantia de que receitas e despesas incorridas são corretamente calculadas, cobradas, pagas e contabilizadas.

Controles Operacionais:

- Monitoramento da conformidade das atividades operacionais em relação aos procedimentos previstos nas políticas internas;
- Monitoramento das informações cadastrais de clientes e da prevenção à lavagem de dinheiro e ao financiamento do terrorismo;
- Segurança da informação, principalmente quanto ao gerenciamento de acessos e senhas e à manutenção de sistemas com trilhas de auditoria;
- Controles que garantam a efetividade do plano de contingência, com acompanhamento e avaliação das atualizações e dos resultados dos testes em relação aos objetivos estabelecidos.

6.8 Perdas Operacionais

O Festor deve desenvolver e manter uma base de dados que contenha valores associados a perdas operacionais, incluindo o evento da perda, provisões e despesas relacionadas a cada evento e demais dados correlatos. A definição de perda operacional está relacionada ao valor quantificável associado aos eventos de controles e seus riscos. Devem ser abertas contas que registram contabilmente as eventuais perdas e/ou prejuízos (provisões e despesas) operacionais, estabelecidas no plano de contas COSIF.

Esta base de dados deve ser resultado das atribuições do gerenciamento de Risco Operacional e da gestão de Controles Internos, sendo fonte de informações para os relatórios gerenciais que devem incluir informações referentes às perdas relevantes. As informações e registros de perdas operacionais devem ser mantidos em documentos originais e/ou arquivos eletrônicos, conforme prazos e responsabilidades estabelecidos pela legislação vigente.

Devem permanecer à disposição do Banco Central do Brasil pelo prazo de 5 (cinco) anos: o Relatório de avaliação de efetividade do Sistema de Controles Internos; e os Planos de Ação e o relatório de acompanhamento pertinente à avaliação de efetividade.

6.9 Dicionário de Riscos — Quadro Resumo

Categoria	Evento	Descrição
Risco Operacional	Fraudes internas	Possibilidade de perda por atos realizados com a intenção de fraudar, subtrair propriedade alheia ou infringir regras, leis ou políticas internas, envolvendo pelo menos um Colaborador.
Risco Operacional	Fraudes externas	Possibilidade de perda por atos realizados por pessoas alheias à organização com a intenção de fraudar, apropriar-se indevidamente de propriedade alheia ou infringir leis.
Risco Operacional	Demandas trabalhistas e segurança deficiente do local de trabalho	Possibilidade de perda por práticas incompatíveis com leis ou acordos trabalhistas, saúde e segurança no ambiente de trabalho, ou pagamentos de reclamações por danos pessoais.
Risco Operacional	Práticas inadequadas relativas a usuários finais, clientes, produtos e serviços de pagamento	Possibilidade de perda por falhas não intencionais ou negligência no cumprimento de obrigação profissional para clientes específicos, ou da natureza de um produto.
Risco Operacional	Danos a ativos físicos	Possibilidade de perda ou danos em ativos físicos em virtude de desastre natural ou outros eventos de grande relevância.
Risco Operacional	Interrupção das atividades ou descontinuidade dos serviços de pagamento	Possibilidade de perdas associadas à interrupção das atividades da instituição.
Risco Operacional	Falhas em sistemas, processos ou infraestrutura de TI	Possibilidade de perdas associadas a falhas em sistemas, processos ou infraestrutura de tecnologia da informação.
Risco Operacional	Falhas na execução, cumprimento de prazos ou gerenciamento de atividades (incl. arranjos de pagamento)	Possibilidade de perda por problemas no processamento e gerenciamento de processos, ou nas relações com parceiros comerciais, vendedores e fornecedores.
Risco Operacional	Falhas na proteção e segurança de dados sensíveis	Possibilidade de perda por problemas no processamento de dados de clientes/usuários.
Risco Operacional	Falhas na identificação/autenticação do usuário final em transação de pagamento	Possibilidade de perda por problemas de processamento na identificação do usuário na transação.

Categoria	Evento	Descrição
Risco Operacional	Falhas na autorização das transações de pagamento	Possibilidade de perda por problemas na autorização de transações.
Risco Operacional	Falhas na iniciação de transação de pagamento	Possibilidade de perda por problemas na iniciação da transação de pagamento.
Risco de Liquidez	—	Possibilidade de perdas pôr o Festor não ser capaz de honrar eficientemente suas obrigações correntes e futuras, ou de não converter moeda eletrônica em moeda física/escritural no momento solicitado.
Risco de Crédito	—	Possibilidade de perdas associadas ao não cumprimento de obrigações financeiras por contrapartes, à desvalorização de instrumentos financeiros, e ao inadimplemento em operações de meios de pagamento e interoperabilidade.
Risco de Mercado	—	Possibilidade de perdas resultantes de flutuação nos valores de mercado de instrumentos detidos pelo Festor (ex.: taxas de juros, ações, câmbio).
Risco de Gerenciamento de Capital	—	Possibilidade de perdas resultantes do gerenciamento ineficiente do capital mantido pelo Festor em relação ao necessário para fazer face aos riscos e ao planejamento estratégico.
Risco de Conformidade	—	Possibilidade de o Festor sofrer sanções legais ou administrativas, perdas financeiras, danos de reputação, decorrentes de descumprimento do arcabouço legal, regulatório ou de autorregulação.
Risco Cibernético	—	Possibilidade de perdas associadas a falhas em procedimentos de segurança cibernética (autenticação, rastreabilidade, controles de acesso, vulnerabilidades, vazamento de informações).
Risco Social, Ambiental e Climático	—	Possibilidade de perdas resultantes de danos sociais, ambientais e climáticos gerados ou sofridos pelas atividades econômicas do Festor.

7. Processo de Compliance

O processo de compliance do Festor é segmentado em quatro etapas, que se integram ao Sistema de Controles Internos descrito na Seção 6:

7.1 Identificação

O risco de compliance refere-se ao risco legal de sanções regulatórias, de perda financeira ou de reputação, resultantes de falhas no cumprimento de leis, códigos de conduta, regulamentações, autorregulamentações, políticas e procedimentos internos e boas práticas — englobando matérias como segregação de funções, conflitos de interesses e princípios éticos.

7.2 Análise

Cabe ao responsável por Compliance, em conjunto com o Comitê de Compliance e Riscos, analisar os casos identificados, considerando a natureza, a gravidade e o contexto de cada situação, conforme as diretrizes de governança descritas na Seção 5.2.

7.3 Tratamento

O tratamento das não conformidades identificadas segue as diretrizes específicas detalhadas nas Seções 8 a 12 desta Política (segregação de atividades e conflitos de interesse, conhecimento do cliente, prevenção à lavagem de dinheiro, combate à corrupção e confidencialidade), bem como o fluxo de Plano de Ação descrito na Seção 6.4.

7.4 Monitoramento e Revisão

A partir do monitoramento, das avaliações e do acompanhamento diário das atividades do Festor, o responsável por Compliance deve identificar deficiências e não conformidades a fim de implementar ações corretivas, comunicando-as ao Comitê de Compliance e Riscos.

Os Colaboradores que identificarem qualquer situação que possa afetar negativamente as atividades e a reputação do Festor devem informar imediatamente o responsável por Compliance, resguardados pela segurança e preservação de sua identidade, sem sofrerem consequências negativas em decorrência dessa atitude.

8. Segregação de Atividades e Conflitos de Interesse

8.1 Segregação de Atividades

O Festor atua como Instituição de Pagamento (IP), possibilitando aos seus clientes realizar movimentações financeiras, pagamentos e demais serviços por meio de instituições financeiras parceiras devidamente conveniadas, dentre outros serviços, sendo suas atividades reguladas pelo Banco Central do Brasil (BACEN).

Deve ser assegurada aos Colaboradores, clientes e às autoridades reguladoras e autorreguladoras a completa segregação de atividades, adotando-se procedimentos operacionais que objetivem tal segregação e evitem possíveis situações de conflito. Todos os Colaboradores devem trabalhar para que suas funções e atividades estejam alinhadas às suas responsabilidades, evitando, ao máximo, situações que possam resultar em conflitos de interesses.

8.2 Conflito de Interesses

Um conflito de interesses inclui qualquer situação na qual um Colaborador esteja envolvido em duas ou mais atividades ou relacionamentos que, em algum grau, sejam incompatíveis, de modo que sua conduta possa conflitar com sua função no Festor ou afetar seu julgamento e desempenho. O conflito de interesse pode surgir quando os interesses pessoais de um Colaborador sejam divergentes ou conflitantes com os interesses do Festor e/ou de seus clientes.

Todo Colaborador deve avaliar, antes de se comprometer em qualquer atividade, função, operação ou relacionamento, se esta ação pode acarretar um conflito. Os Colaboradores têm o dever de agir com boa-fé e de acordo com os interesses dos clientes e do Festor, com o intuito de não ferir a relação fiduciária com eles.

Os Colaboradores ficam proibidos de exercer atividades profissionais externas ao Festor, remuneradas ou não, salvo se previamente aprovadas pelo Comitê de Compliance e Riscos, respeitando sempre que: é proibida qualquer atividade ilícita; é vetado ao Colaborador trabalhar para qualquer concorrente do Festor ou atuar como diretor, representante ou consultor deste; e é vedada a condução de atividades paralelas, inclusive filantrópicas e civis, durante a jornada de trabalho, ou que de qualquer forma afetem o desempenho do Colaborador.

O responsável por Compliance deve fazer parte do Comitê de Remuneração do Festor, com o intuito de monitorar e participar da formulação das políticas de incentivos, de maneira a assegurar que: (i) a política de remuneração do Festor não leve a conflitos com os interesses de clientes; e (ii) taxas, comissões e encargos pagos a terceiros ou recebidos de terceiros não levem a conflitos com os interesses dos clientes.

São exemplos de situações que podem ser caracterizadas como conflito de interesse pessoal e profissional, dentre outras: investimentos pessoais; transações financeiras com clientes fora do âmbito do Festor; recebimento de favores ou presentes de administradores e/ou sócios de empresas parceiras,

fornecedores ou clientes; análise financeira ou operação com empresas cujos sócios, administradores ou funcionários o Colaborador possua relação pessoal ou investimento próprio; e participação em atividade política ou em funções e atividades externas.

9. Conhecimento do Cliente (Know Your Client)

O Festor adota a política de análise e identificação do cliente com o objetivo de conhecê-lo, estabelecendo um conjunto de regras que propiciem identificar e conhecer a origem e constituição de seu patrimônio e recursos financeiros. Os Colaboradores devem cadastrar os clientes previamente ao início da prestação de serviços, de acordo com os procedimentos estabelecidos pelos normativos do BACEN, sendo o cadastro validado e atualizado periodicamente.

O Festor conta com os esforços de todos os Colaboradores e prestadores de serviços para: (i) realizar a identificação de clientes novos ou já existentes e promover sua atualização periódica; e (ii) prevenir, detectar e reportar quaisquer operações suspeitas. O responsável por Compliance deve acompanhar as atividades dos setores integrantes do Festor nesse sentido.

O Festor, com o acompanhamento do responsável por Compliance, deve estabelecer análise independente e assegurar processo reforçado de due diligence com relação às Pessoas Politicamente Expostas ("PEP"), definidas como pessoas que exerceram altos cargos de natureza política ou pública, assim como seus representantes, familiares e outras pessoas de seu relacionamento próximo.

Para o detalhamento completo dos procedimentos de KYC e onboarding, vide a Política de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo do Festor.

10. Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo

Entende-se por lavagem de dinheiro as práticas econômico-financeiras que têm por finalidade dissimular a origem ilícita de determinados ativos, de forma que estes aparentem ter origem lícita. Qualquer suspeita de operações financeiras e não financeiras que possam apresentar indícios ou evidências de envolverem atividades relacionadas aos crimes de lavagem de dinheiro devem ser comunicadas imediatamente ao responsável por Compliance.

Consideram-se atividades suspeitas, entre outras: as que possam estar relacionadas a recursos provenientes de atividades criminosas ou que visem ocultar recursos ou ativos com tal origem; as que possam comprometer recursos utilizados, no todo ou em parte, para atividades de natureza terrorista; as fracionadas ou estruturadas para evitar registros ou comunicações sistemáticas exigidas pela legislação de PLD/FT; as sem finalidade comercial clara ou explicação razoável; e as que envolvam montantes incompatíveis com a ocupação profissional, os rendimentos e/ou a situação patrimonial/financeira das partes envolvidas.

O responsável por Compliance, juntamente com o Comitê de Compliance e Riscos, analisará e conduzirá o caso às autoridades competentes, mediante avaliação dos instrumentos utilizados, a forma de realização, as partes e valores envolvidos, a capacidade financeira e a atividade econômica dos envolvidos, e qualquer indicativo de irregularidade. O Festor compromete-se a comunicar ao COAF (Conselho de Controle de Atividades Financeiras) todas as transações ou propostas que possam constituir indícios de crimes de lavagem ou ocultação de bens, direitos e valores.

O responsável por Compliance deve emitir relatório com periodicidade anual, listando as operações identificadas como suspeitas e as operações ou propostas devidamente comunicadas às autoridades competentes. Os processos de registro, análise e comunicação são realizados de forma sigilosa, inclusive em relação aos envolvidos.

No caso de envolvimento de Colaboradores em operações dessa natureza, estes ficarão sujeitos às penalidades previstas nesta Política, além das consequências legais cabíveis, podendo resultar em desligamento ou exclusão por justa causa (sócio), demissão por justa causa (empregado), ou rescisão de contrato (prestador de serviços).

Cabe ao responsável por Compliance: monitorar e fiscalizar periodicamente o cumprimento, pelos Colaboradores, das regras de combate e prevenção à lavagem de dinheiro; definir políticas,

procedimentos e treinamentos de compliance; acompanhar o desenvolvimento e a implementação de ferramentas de controle nas áreas de negócios, como cadastro de clientes e KYC; e acompanhar sistemas de monitoramento com critérios pré-estabelecidos (limites e movimentações) na área de contas a pagar e a receber.

Para o detalhamento completo desta matéria, vide a Política de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo do Festor, elaborada em conformidade com a Lei nº 9.613/1998 e as normas do BACEN e do COAF aplicáveis.

11. Combate à Corrupção

A Lei Anticorrupção (Lei nº 12.846/2013), vigente desde 1º de agosto de 2013, e seu Decreto Regulamentador nº 11.129/2022, dispõem sobre a responsabilidade civil e administrativa de sociedades brasileiras ou estrangeiras que atuem no Brasil por atos de seus diretores, gerentes, funcionários e outros agentes que envolvam a prática de corrupção contra a administração pública, nacional ou estrangeira, inclusive organizações públicas internacionais, como suborno e fraude em licitações e contratos administrativos.

Nos termos das normas acima mencionadas, suborno significa prometer, oferecer ou dar, direta ou indiretamente, vantagem indevida a agente público, ou a terceira pessoa a ele relacionada, incluindo os chamados "pagamentos facilitadores". Corrupção compreende qualquer ato de se corromper, oferecer algo para obter vantagem em que se favorece uma pessoa e se prejudica outra, incluindo atos ilegais caracterizados por falsidade, encobrimento ou violação da confiança.

Os Colaboradores do Festor, sempre que perceberem algum ato com suspeita ou confirmação de corrupção, devem comunicar imediatamente o responsável por Compliance. Os atos podem envolver parceiros externos, clientes ou potenciais clientes.

12. Segurança, Segurança da Informação e Segurança Cibernética

As medidas de segurança, segurança da informação e segurança cibernética têm por finalidade minimizar as ameaças aos negócios e atividades do Festor, ao sigilo de dados de Colaboradores, clientes e fornecedores, e garantir a integridade funcional do parque tecnológico da Companhia. O detalhamento completo dos princípios, papéis, responsabilidades e controles técnicos aplicáveis consta na Política de Segurança da Informação e Cibernética do Festor, elaborada em conformidade com a Resolução BCB nº 85/2021 e a LGPD, à qual esta Política se remete integralmente.

Sem prejuízo do disposto na política específica, destacam-se as seguintes diretrizes gerais de conduta, aplicáveis a todos os Colaboradores:

- Documentos sensíveis devem ser retirados da mesa e armazenados em gavetas ou armários quando o Colaborador se ausentar por períodos prolongados, mantendo-se a Política de Mesa Limpa ao final do expediente;
- É proibida a cópia (física ou eletrônica) de arquivos da rede do Festor para circulação em ambientes externos sem objetivo relacionado às funções do Colaborador e sem autorização prévia;
- Documentos físicos com informações confidenciais devem ser triturados e descartados imediatamente após seu uso, de maneira a evitar sua recuperação ou leitura;
- É proibida a conexão de equipamentos externos (pendrives, HDs externos etc.) na rede do Festor sem vinculação com a função do Colaborador e sem prévia autorização;
- A utilização de computadores, notebooks, telefones, internet, e-mail e demais equipamentos do Festor destina-se exclusivamente a fins profissionais;
- É terminantemente proibido o envio, repasse ou visualização de conteúdo discriminatório, preconceituoso, obsceno, pornográfico ou ofensivo por qualquer meio corporativo;
- Senhas e logins são pessoais e intransferíveis, não devendo ser divulgados a terceiros sob nenhuma hipótese;

- Computadores e arquivos de e-mail corporativos poderão ser inspecionados pelo Festor a qualquer tempo, por meio do responsável por Compliance, para verificação da observância desta Política.

13. Plano de Continuidade de Negócios

O objetivo do Plano de Continuidade de Negócios do Festor é estabelecer as medidas e a estrutura do plano de resposta a ser adotado em momentos de crise que acarretem, ou possam vir a acarretar, descontinuidade das atividades operacionais indispensáveis ao bom funcionamento da instituição.

O Colaborador responsável pela coordenação das atividades e da comunicação em situações contingenciais é o responsável por Riscos e Compliance ou, na sua ausência, os gestores de cada área. Em situações de impossibilidade de acesso às instalações físicas, todos os Colaboradores deverão se dirigir aos gestores responsáveis pela continuidade operacional. Outros fatores que podem motivar o acionamento do plano de contingência incluem problemas técnicos (falhas de hardware e software), ausência de pessoas-chave, e crises de infraestrutura.

Em situações de risco, o responsável pelo setor de Riscos e Compliance deve: compreender a natureza do risco e avaliar as diferentes formas de impacto negativo; definir as medidas a serem tomadas para mitigar os impactos e garantir o bom funcionamento e atendimento a clientes; contatar os Colaboradores de forma geral e individualizada, conforme prioridades definidas; acompanhar as atividades até a retomada operacional; e analisar e avaliar o ocorrido após sua conclusão, propondo melhorias para situações semelhantes futuras.

Para o detalhamento técnico completo (planos de recuperação de desastres, RTO/RPO, testes de continuidade), vide a Política de Segurança da Informação e Cibernética do Festor e o Plano de Continuidade de Negócios específico.

14. Confidencialidade

Os Colaboradores do Festor serão frequentemente expostos a informações confidenciais relacionadas ao negócio, incluindo informações a respeito da própria instituição, de seus clientes, parceiros comerciais e fornecedores, e informações relativas aos demais Colaboradores.

Nenhuma informação confidencial deve, em qualquer hipótese, ser divulgada fora do ambiente do Festor, fornecida ao público, à mídia ou a demais órgãos, sem a devida autorização do Comitê de Compliance e Riscos. São consideradas informações confidenciais, por exemplo: processos, metodologias, modelos e sistemas do Festor e de parceiros; informações técnicas, financeiras e comerciais; e estratégias de abertura de contas, gestão, política de crédito, saldos, extratos, posições de clientes e operações estruturadas.

Princípios a serem observados pelos Colaboradores ao lidar com informações: todas as informações devem ser consideradas confidenciais, seja em formato escrito, verbal ou eletrônico; informações pessoais a respeito de indivíduos devem ser tratadas como confidenciais; e deve-se comentar ou fornecer informações relacionadas ao negócio somente se fizer parte da função do Colaborador ou com autorização — em caso de dúvida, consultar o responsável pela área de Compliance.

Considera-se informação privilegiada aquela informação relevante e material a respeito de qualquer companhia, produto e/ou serviço, que não tenha sido divulgada publicamente e que tenha sido obtida de forma privilegiada — devendo ser mantida em sigilo por todos que a ela tiverem acesso, seja em decorrência do exercício da atividade profissional ou de relacionamento pessoal.

15. Programas de Treinamento

O Festor executa um processo de treinamento inicial para todos os Colaboradores no ingresso na organização, com maior foco àqueles em gestão de riscos e operações, em especial os que tenham acesso a informações confidenciais. O treinamento inicial aborda as atividades do Festor, a regulamentação e autorregulamentação aplicável, as regras relativas à atividade desenvolvida, o perfil dos clientes, e as políticas, procedimentos e processos internos.

O Festor entende que é fundamental que todos os Colaboradores, especialmente aqueles com acesso a informações confidenciais, tenham conhecimento atualizado dos princípios éticos e das leis, regulamentações e normas relevantes, adotando um programa de reciclagem periódica na medida em que as regras e conceitos tratados nesta Política sejam atualizados.

16. Responsabilidades

Área/Papel	Responsabilidades
Diretoria Executiva	Garantir a promoção de elevados padrões éticos e de integridade; estabelecer cultura organizacional com ênfase na relevância dos sistemas de controles internos e no engajamento de cada Colaborador; manter estrutura organizacional adequada para garantir a qualidade e a efetividade dos sistemas e processos de controles internos; e prover recursos adequados e suficientes para o exercício das atividades relacionadas ao sistema de controles internos, de forma independente, objetiva e efetiva.
Diretoria de Riscos e Controles	Responder perante o Banco Central do Brasil pelas atribuições de Controles Internos; prover os meios necessários para o exercício adequado das atividades de Controles Internos; implementar as diretrizes relativas aos sistemas de controles internos aprovadas pela Diretoria Executiva; e monitorar a adequação e a eficácia do Sistema de Controles Internos.
Área de Controles Internos	Implementar e operacionalizar indicadores de controles junto aos processos/subprocessos do Festor; testar e avaliar a aderência aos indicadores de controle, de acordo com as recomendações dos órgãos reguladores e o Código de Ética e Conduta; revisar e acompanhar a solução dos posicionamentos levantados em relatórios de auditoria; desenvolver e ajustar, em conjunto com as áreas institucionais, indicadores de controles; e elaborar relatório, com periodicidade mínima anual, contemplando o sumário dos resultados das atividades e suas principais conclusões.
Gestão de Riscos	Acompanhar os processos e controles internos de forma independente; avaliar a eficácia do gerenciamento de riscos e dos controles internos; e propor ajustes no Sistema de Controles Internos.
Auditoria Interna	Auditar os processos e controles internos de forma independente, anualmente; prover avaliações sobre a eficácia do gerenciamento de riscos e dos controles internos; e apresentar Relatório de Auditoria à Diretoria Executiva.
Dono do Processo	Controlar e mitigar os riscos relativos às atividades sob sua responsabilidade, implementando, quando necessário, planos de ação e procedimentos formalizados e aderentes às obrigações legais e regulatórias; envolver a área de Controles Internos sempre que tiver ciência de fato que possa expor o Festor a riscos; e assimilar e disseminar a cultura de Controles Internos.
Responsável por Compliance	Conforme detalhado na Seção 5.2 desta Política.
Comitê de Compliance e Riscos	Conforme detalhado na Seção 5.2 desta Política.

17. Penalidades

Violações a esta Política devem resultar em advertência, revisão de responsabilidade, suspensão ou dispensa, conforme o caso, do contrato de trabalho e/ou de prestação de serviços, por recomendação do responsável por Compliance ou de qualquer dos diretores responsáveis, submetidas primeiramente ao Comitê de Compliance e Riscos e à posterior decisão final da Diretoria Executiva.

O Festor não assume a responsabilidade por Colaboradores que transgridam a lei ou cometam infrações no exercício de suas funções. Caso o Festor venha a ser responsabilizado ou sofra prejuízo de qualquer natureza por atos de seus Colaboradores, poderá exercer o direito de regresso em face dos responsáveis.

O Colaborador que tiver conhecimento ou suspeita de ato não compatível com os dispositivos desta Política deve reportar imediatamente tal acontecimento ao responsável por Compliance. O Colaborador que se omitir dessa obrigação poderá sofrer, além de ação disciplinar, rescisão de contrato ou demissão por justa causa. Colaboradores que, de boa-fé, reportarem uma possível violação devem ser protegidos e não sofrerão qualquer penalidade.

18. Canais de Comunicação / Canal de Denúncias

Informe sempre, de forma tempestiva, qualquer violação suspeita ou real de eventos ou informações do Festor, pelos seguintes canais:

Canal	Contato
E-mail de Compliance	compliance@grupofestor.com.br
E-mail de Privacidade	dpo@grupofestor.com.br
Canal de Denúncias	https://grupofestor.com.br/canal-de-denuncias/
Site institucional	www.grupofestor.com.br

19. Revisão

O Festor e o ambiente no qual atua são dinâmicos. Para assegurar que evoluções sejam incorporadas a esta Política continuamente, refletindo as melhores práticas de mercado e da Companhia, as revisões devem ser efetuadas com periodicidade mínima anual, ou sempre que houver alteração relevante na regulamentação do BACEN ou de demais órgãos reguladores.

A responsabilidade pela elaboração e atualização desta Política é da área de Compliance do Festor, que encaminhará proposta formal para avaliação e aprovação do Comitê de Compliance e Riscos e posterior avaliação e aprovação da Diretoria Executiva.

Data da última atualização: 14 de agosto de 2026.

Anexo I. Histórico de Versões

Versão	Data	Produzido	Autorizado	Conteúdo
1.0	20/03/2023	Compliance	Diretoria Executiva	Estruturação inicial como Política de Controles Internos & Compliance.
2.0	04/07/2024	Compliance	Victor Volpato / Luís Antônio Dias Soares / Pedro Zuaid Dias Soares	Reestruturação como Manual de Controles Internos, com metodologia de Matriz de Riscos e Controles (MRC), alinhada à Resolução BCB nº 260/2022.
3.0	16/08/2024	Compliance	Victor Volpato / Luís Antônio Dias Soares / Pedro Zuaid Dias Soares	Revisão periódica da metodologia de controles internos.
4.0	14/08/2026	Compliance / Controles Internos e Riscos	Diretoria Executiva	Fusão das versões anteriores em documento único; atualização de razão social, CNPJ e endereço para Festor Instituição de Pagamento Ltda.; incorporação dos processos de compliance à estrutura de controles internos; alinhamento visual ao padrão de governança do Festor.